Menya

Communications Ltd.

Agile vs. Cyber

Samuel Wanderi MSIM CAIS CISSP CCNA GSLC CEH COR

AGILE Development

Cyber Security

Agenda

- Overview of Industry Direction
- AGILE in DoD
- Cyber in DoD
- People Solutions
- Process Solutions
- Technology Solutions

DOD Direction

- Providing the Warfighter's Edge (Lt Gen JT Thompson AFLCMC)
  - Aircraft Structural Integrity Program (ASIP)
  - Teaming/Relying on each other
  - Cyber resiliency of weapon systems

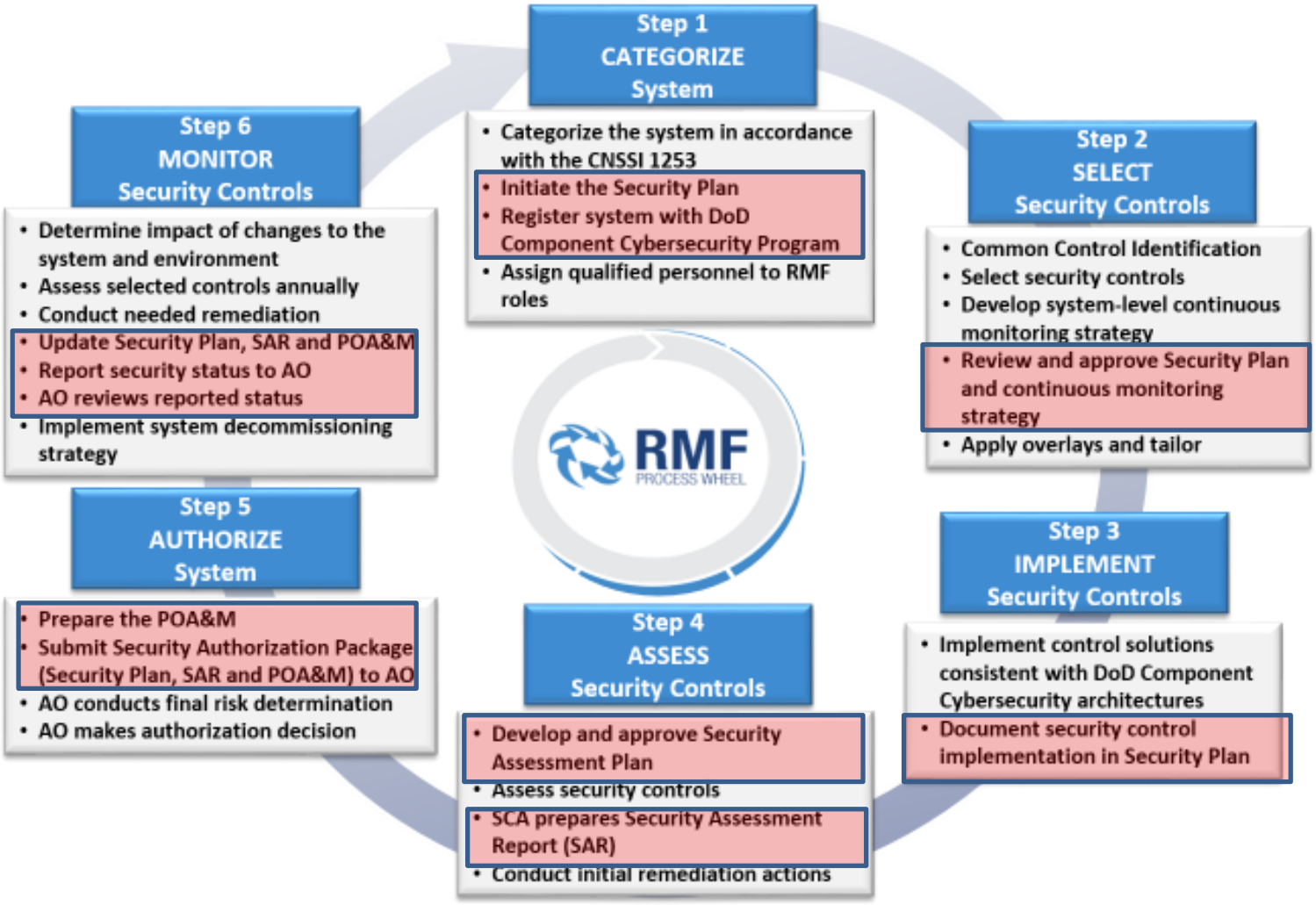
- Keeps me up at night (B Gen Anthony Genatempo F22)

  Competition: Sukhoi PAK FA T-50; Chengdu J-20

  Who can deliver faster - AGILE (MOD development)

- Stay ahead of Adversary
  - Increase Resiliency
  - Increase Adaptability
  - Increase Security or Reduce Risk

Cyber Security Direction



AGILE Manifesto Direction

Pro

- *Individuals and interactions*
- *Working software*
- *Customer collaboration*
- *Responding to change*

Con

- *Processes and tools*
- *comprehensive documentation*
- *contract negotiation*
- *following a plan*

That is, while there is value in the items on the right, we value the items on the left more."

AGILE & Cyber Challenges

- The pressure of short iteration (Bartsch, 2011) (Securosis, 2013).
- Lack of information security knowledge (Securosis, 2013)
- Lack of security awareness (Bartsch, 2011)
- In-compatibility of security activities and agile methodologies (Keramati & Mirian-Hosseinabadi, 2008)

Solutions

- Must Face Reality (Myth Busting)
  - Fight the Fight not the Plan
  - Cyber is Crime (No Quick Fixes)
  - Current Cyber Process is Linear not AGILE
  - Cyber is bigger than IT & Engineering
- Systemic Changes is Needed
  - People
  - Process
  - Technology

People Changes

Super Hackers

Vs

The **Real** World

^


MR. ROBOT


BOOK
SIGNING
Kevin Mitnick
KEVIN MITNICK
GHOST
IN THE
WIRES


www.mugshots.com
WANTED
BY U.S. MARSHALS


FROM MICHAEL MANN DIRECTOR OF HEAT, COLLATERAL AND THE INSIDER
CHRIS HEMSWORTH
blackhat
WE ARE NO LONGER IN CONTROL
JANUARY 16 2015
OFFICIAL SITE
DOWNLOAD PHOTOS
#blackhat
WATCH THE NEW TRAILER
R
LEGENDARY
UNIVERSAL

Cyber (REAL World)

- Standards:
  - ETSI Cyber Security Technical Committee (TC CYBER)
  - ISO 27001 and 27002
  - Standard of Good Practice
  - NERC
  - NIST - National Institute of Standards and Technology
  - ISO 15408
- Not Enough Professionals to go around
- Cyber Professionals also have Strengths and Weaknesses
- Continuous Testing & Training for everyone
- Cyber Hygiene - everyone has to be involved


SYS. mmHg
DIA. mmHg
Pulse/min
INFLATE AIR
DEFLATE AIR
REPLACE BATTERIES
LAST MEASUREMENT
MEMORY
M
S
I.U.

Highest Paying Certifications

2017

1. Citrix Certified Professional – Virtualization (CCP-V)
2. Project Management Professional (PMP)
3. Certified Information Systems Auditor (CISA)
4. Certified Information Systems Security Pro (CISSP)
5. AWS Certified Solutions Architect – Associate
6. Certified Information Security Manager (CISM)

2016

1. AWS Certified Solutions Architect – Associate
2. Certified in Risk and Information Systems Control (CRISC)
3. Certified Information Security Manager (CISM)
4. Certified Information Systems Security Professional (CISSP)
5. Project Management Professional (PMP®)
6. Certified Information Systems Auditor (CISA)

Trend holds true in 2013, 2014, 2015

PCMag.com

Table AP3.T2. DoD Approved Baseline Certifications

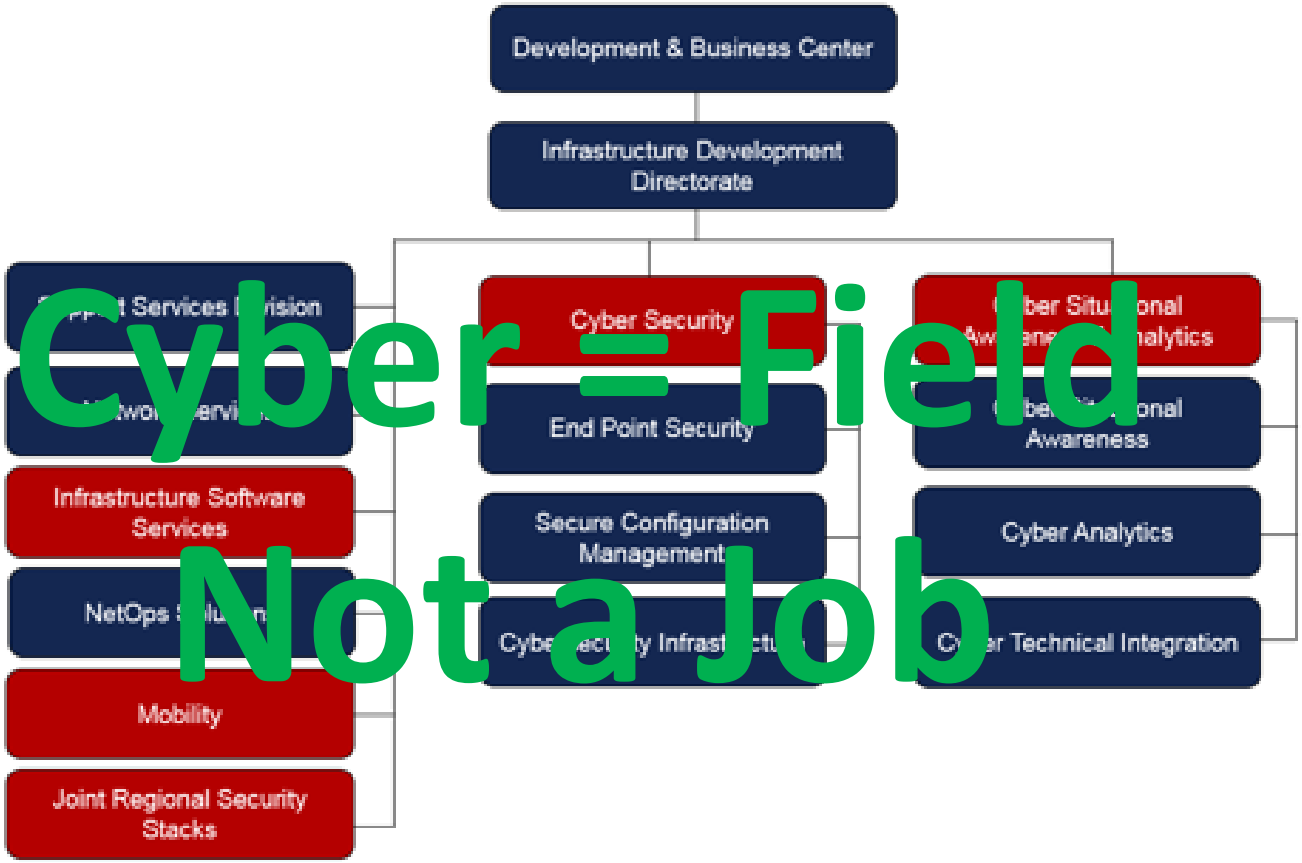
IAT Level I	IAT Level II	IAT Leve III
A+-CE	GSEC	CISA GCIH
Network+CE	Security+CE	GCED
SSCP	SSCP	CISSP (or Associate)
CCNA-Security	CCNA-Security	CASP

IAM Level I	IAM Level II	IAM Level III
CAP	CAP	GSLC
GSLC	GSLC	CISM
Security+CE	CISM CASP	CISSP (or Associate)
	CISSP (or Associate)	

IASAE I	IASAE II	IASAE III
CISSP (or Asociate)	CISSP (or Associate)	CISSP-ISSEP
CASP	CASP	CISSP-ISSAP
CSSLP	CSSLP	

CNDSP Analyst	CNDSP Infrastructure Support	CNDSP Incident Reporter	CNDSP Auditor	CNDSP Manager
GCIA	SSCP	GCIH	CISA	CISSP-ISSMP
CEH	CEH	CSIH	GSNA	CISM
GCIH		CEH GCFA	CEH	

Cyber Org Chart Example (DISA)



NIST 800-53A

Assessment Methods

Examine - process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities).

Interview - process of holding discussions with individuals or groups of individuals within an organization

Test - process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

Audit Only

Planning Factors

Industry Controls / Level of Effort = Time

Example:

If 1 Person = 4 Controls / Week

400 Controls / 1 Person = 100 Weeks ~ 2 Years

Secure AGILE Processes

- Scrum
  - The Security Sprint Approach
  - Every-Sprint approach
  - S-Scrum “Spikes”
  - Secure Scrum
- Extreme Programming
  - SQUARE (Security Quality Requirements Engineering)
- Dynamic Systems Development Method
  - Role-based Extreme Programming (XP) for Secure Software Development

AGILE Documentation Myth

"But Agile is not an excuse for skipping documentation—especially important security artifacts."

"Documentation is just as important in Agile projects, though it is often more focused and condensed."

AGILE IS FRAGILE

By Peter T. Davis, CISA, CISM, CGEIT, COBIT Foundation, COBIT Implementation, COBIT Assessor, COBIT INCS, CISSP, CPA, CMA, CMC, ITIL FC, ISO 9001 FC, ISO 20000 FC/LI/LA, ISO 27001 LI/LA, ISO 27005/31000 RM, ISO 28000 FC, ISTQB CTFL, Lean IT FC, Open FAIR FC, PMI-RMP, PMP, PRINCE2 FC, SSGB, RESILIA FC

The Nexus | 8 February 2016

Process Conclusions

- Security is not inherent in AGILE
- Minimize not eliminate documentation
- More SME’s or more time for security
- Current security process is liner
- No quick fixes or shortcuts
- Addressing security up front is most effective

AGILE Cyber Technology

GSA has been working with the Office of American Innovation (OAI) and American Technology Council to **improve the process** to achieve an Authority to Operate (ATO) alone the following dimensions:

- **Reducing toil** that inhibits our ability to scale improvements
- **Decreasing errors** from manual activities
- **Increasing speed** to process (approvals and identification of issues)
- Increasing value-add of machine-readable data for **improving risk management**

One key component of this effort is identifying ways to incorporate **automation** into the ATO process. To assist agencies and industry collectively, GSA would like to have a better understanding of the existing commercially available products, and practices, that the government could use to **automate** any portion of the ATO process

AGILE Cyber Technology

Name	Vendor	Features	Compliance
CSET(Cyber Security Evaluation Tool)	ICS-CERT	CSET contributes to an organization's risk management and decision-making process. Raises awareness and facilitates discussion on cybersecurity within the organization. Highlights vulnerabilities in the organization's systems and provides recommendations on ways to address the vulnerability. Identifies areas of strength and best practices being followed in the organization. Provides a method to systematically compare and monitor improvement in the cyber systems. Provides a common industry-wide tool for assessing cyber systems There is no information about automation of the process There is need for trained workforce to do the evaluation and from various disciplines Questionnaire to be answered by the organization to have the evaluation result to be available	NERC, NIST 800-82, NIST 800-53, NIST Cybersecurity Framework
Software Assessment Questionnaire	Qualys	Transformative cloud solution (SaaS) for automating and streamlining an organization's vendor risk management process SAQ's wizard and its simple, drag-and-drop web UI captures responses in real time and aggregates them in one central dashboard, so administrators can see campaigns' progress Require that respondents attach evidence files for certain answers Allow respondents to delegate questions to peers that are better able to answer them	NIST, HIPAA, SOX, PCI
ZenGRC	Reciprocity Labs	Easily manage compliance across multiple standards Replace spreadsheets with an all-in-one GRC tool Track and map policies, controls, risks, vendors, and more Centralize evidence collection and assessments Monitor assessment activities with full event tracking Assign and control access with full Role Based Access	ZenGRC has FedRAMP and NIST SP 800-53 controls pre-loaded in the tool
Logic Manager ERM	Logic Manager	Software as a Service Out -of the box industry specific templates IT Professional team not required Can be configured by business admin Enterprise risk management and compliance check Vendor management and manage regulations with built in libraries	It comes with NIST Cybersecurity framework and NIST 800-171
Risk Manager Module	Modulo	Automation of risk assessments Automate compliance assessment with various regulations required Quick charts and stats generation	COBIT, ITLI, PCI DSS, ISO 27001 NBR 15999
IT Audit Machine	ContinuumGRC	Many of the clients are federal organizations such as DHS and international government agencies Automated reporting Has both self use tool and services provided by the vendor capability	FedRAMP, FISMA, DoD, and NIST
Vendor Assessment Program	DatumSec	Automated assessment of all the clients An assessment can be used for multiple clients without the hassle of completing separate questionnaire Generate real-time views of how and where your systems and data are at risk DatumSec's vulnerability, policy and configuration assessments are based on NIST, SANS and other risk-management standards and best practices	NIST, SANS

Sam@MenyaLTD.com

937-567-0757